Handling Risk in Electronic Reporting Programs

Everyone knows the burdens imposed on businesses by government paperwork—the hours spent gathering data and filling out forms to comply with state and federal laws. But what's happening at the other end of that transaction? In Ohio, the state receives more than 25,000 pages of data every month on pollution discharges to its surface waters. That's well over a quarter million pages a year in one regulatory program alone, all of which must be received, checked for errors, and entered manually into a computer database.

Electronic reporting addresses this burden by enabling states and regulated facilities to exchange data as computer files, which can be processed with minimal human intervention and at much greater speed than ever before. States have adopted electronic reporting in various regulatory programs over the past several years and have experienced substantial increases in efficiency while saving agency resources.

To date, most state electronic reporting programs have concentrated on a single reporting requirement or a single media program. However, to increase the benefits of electronic reporting, states have begun to implement systems that integrate information collection throughout their environmental agencies. Such systems not only increase the efficiency of agency data collection, but are also an integral part of plans to allow agencies seamless access to all of their data, regardless of what department originally collected it.

Designing and implementing an effective electronic reporting program is a complex undertaking, one that will rarely come out perfect the first time. States need room to experiment with different approaches and must maintain a willingness to revise the system as appropriate in response to new developments and new technologies. Although much can be accomplished through pilot programs, it is likely that most problems in a system will only be found through general use.

The newness and complexity of electronic reporting combine to create a degree of risk in the implementation of these programs. This does not mean that electronic reporting should never be attempted—any move away from the tried and true involves risk. Instead, agencies must plan for the risks they can identify but not eliminate, use other aspects of the system to mitigate these risks as much as possible, and adjust the system when future developments make these risks reach an unacceptable level.

Planning for risk needs to begin at the earliest design stages. What constitutes a risk depends heavily on the person identifying it, so it is important to get input from all those affected by the system, including enforcement personnel and regulated facilities. For example, industry sometimes sees the electronic transfer of business information as a significant risk unless steps are taken to safeguard the transmission.

Simplicity is the key to designing an effective electronic reporting system and reducing risk. Not only are simple systems easier to manage, they are easier to explain to users and in court. This leads to a higher level of participation in the program, particularly among smaller reporting entities.

Once risks have been identified, it should be determined what steps will be necessary to either eliminate them completely or reduce them to an acceptable level. Although in some cases the risk may be eliminated quite easily, in others it would be prohibitive in terms of cost or system complexity to achieve that goal. In such cases it may be possible to balance the risk through benefits provided by other aspects of the system. When the risk cannot be reduced to an acceptable level, it may be better to limit participation in the electronic reporting program to limited groups where the risk cam be managed or to specific reporting requirements where the risk is not as strong.

After the system has been running for a while, it will be tested through use of the data it collects for various agency activities. With good planning and design, all will go well and these events will become evidence of the system's reliability. However, these developments could expose flaws in the agency's efforts to eliminate or control risk, or even uncover unforeseen risks. The only solution to the situation is the ability to change the system as necessary. An electronic reporting program cannot be set in stone, it needs to be evaluated constantly by both regulators and reporters if it is to handle these risks and take advantage of rapidly changing technology. In extreme cases, an agency must be willing to admit that a system is not working and begin again.

The importance of thoughtful design can be clearly seen in one of the more significant risks associated with electronic reporting—identifying the specific individual responsible for an electronic submission. Without a signature in hand and lacking case law in this area, some environmental prosecutors worry that it will be difficult to convince juries to criminally convict an individual for false reporting of data. They are particularly concerned about password based identification systems, which are not strongly tied to an individual because the password can be easily shared.

However, the electronic signature solutions generally offered to solve this problem, such as public key cryptography or biometrics, have their own drawbacks. Such systems are generally expensive to implement. They are unfamiliar to the general public and would require extensive expert testimony to convince juries of their effectiveness. These systems are often complex, offering a wealth of opportunities for defense attorneys to raise doubts about how they function. As one state attorney said to me, "Prosecutors thrive on simplicity; defense counsel revels in complexity."

The ultimate determination of how to best address this issue will turn on the risk it poses for specific uses of an electronic reporting system. No matter what identification method is used, the risk of losing criminal prosecutions will still exist. To eliminate it, an agency must either forgo electronic reporting or require parallel paper submissions. For those willing to accept a degree of risk, it may be best to begin with a simple system that produces reliable data, adding layers of complexity only as justified by specific court cases. In general, states only proceed with criminal prosecutions when they have overwhelming evidence of wrongdoing and feel that the risk of losing cases due to signature issues is small. This risk is somewhat controlled by the fact that electronic reporting produces better quality data that is available faster, enhancing the other evidence used in the case. In those cases where a criminal prosecution fails, states still have access to other sanctions that can have significant effects on the individual and facility responsible for the report.

Jim Whitter is a Policy Analyst for the National Governors' Association Center for Best Practices. He is also co-chair of the State Electronic Commerce and EDI Steering Committee, a group of state and federal officials who have written a guide to help states develop effective electronic reporting programs, due to be published this Fall.